



Scott Tischler

FOUNDER & CHAIRMAN · AIRECOMMEND.AI

AI & SEARCH

# What Is MCP (Model Context Protocol)? AI Agents' Plumbing, Explained for Business Owners

By Scott Tischler · July 30, 2026 · 8 min read

---

There's a piece of technology quietly reshaping how AI works with the real world, and most business owners have never heard its name. It's called **MCP — the Model Context Protocol** — and it's the plumbing that lets AI agents connect to actual tools and live data instead of guessing from stale text.

I get why this one flies under the radar. It sounds deeply technical, like something only engineers need to care about. But I'll make the case that MCP matters to you the same way the plumbing behind your walls matters: you don't need to be a plumber, but if you ignore it, nothing flows. Let me explain what it is, why it exists, and what it practically means for how your business shows up to AI.

## What is MCP, in one plain sentence?

**MCP is an open standard that gives AI agents a consistent, secure way to connect to external tools and data sources.** Think of it as a universal adapter between an AI model and everything outside it — your inventory system, your booking calendar, your product catalog, a spreadsheet, a database.

The analogy I use with clients: MCP is like **USB-C for AI**. Before USB-C, every device needed its own special cable, and nothing was interchangeable. MCP does for AI connections what USB-C did for chargers — one standard way to plug an AI agent into a tool, so any compliant agent can talk to any compliant data source without a custom integration built from scratch each time.

That's the whole idea. Introduced as an open standard and gaining real adoption through 2026, MCP is becoming the common language for how AI agents reach the tools and information they need to actually **do** things rather than just talk about them.

## Why does MCP exist? The problem it solves

To see why MCP matters, you have to understand a limitation of AI models on their own. A language model is trained on data up to a point in time and then frozen. Left alone, it doesn't know your current prices, today's inventory, or whether a table is free tonight. It can sound confident and still be wrong or out of date.

For years the workaround was **custom integrations** — a developer hand-builds a bridge between one AI system and one tool. That works, but it's the "special cable for every device" problem. Every combination of AI and tool needed its own bespoke connection: expensive, brittle, and impossible to scale. If you wanted your data available to three different AI systems, that was potentially three separate builds.

MCP replaces that mess with one protocol. A business exposes its data or capability once, through an **MCP server**, and any AI agent that speaks MCP can connect to it — with permissions and boundaries you control. Fewer custom builds, more interoperability, and crucially, **live** data instead of frozen guesses.

Here's the simple contrast:

|                | Before MCP                         | With MCP                         |
|----------------|------------------------------------|----------------------------------|
| Connections    | Custom-built for each AI-tool pair | One standard interface           |
| Data freshness | Often stale or model-trained       | Live, real-time                  |
| Scaling        | New integration per system         | Expose once, many agents connect |
| Control        | Ad hoc, varies by build            | Defined permissions and scope    |
| Cost           | High developer overhead            | Sharply lower over time          |

## How MCP actually works (without the jargon)

Let me keep this concrete. MCP has two sides:

- **An MCP client** — this lives inside the AI application or agent (for example, an AI assistant a customer is using).
- **An MCP server** — this is what a business or tool provider runs to expose specific data or actions.

When the agent needs something — your live product availability, say — its MCP client asks your MCP server, which responds with structured, current information, or performs an allowed action like checking a booking. You decide exactly what the server exposes: which data, which actions, and under what limits. It's not a firehose to your whole system; it's a controlled window you define.

Three kinds of things a server can offer:

1. **Resources** — data the agent can read (a catalog, documents, records).
2. **Tools** — actions the agent can take (check availability, create a booking, look up an order).
3. **Prompts** — reusable templates that guide how the agent uses the above.

The takeaway for a non-technical owner: MCP is how an AI agent stops guessing about your business and starts working with your **actual**, current information — within rules you set.

## Why should a business owner care?

Because MCP sits directly on the fault line I keep pointing my clients to: the shift from AI that **describes** the world to AI that **acts** in it. This is the same shift powering **agentic commerce** — AI agents that browse, choose, and even buy on a person's behalf. Those agents are far more useful, and far more accurate about you, when they can reach live data through MCP.

Consider what "connected" versus "disconnected" looks like:

- **Disconnected:** an AI assistant answers a customer's question about your business from stale training data or a cached page. It might quote an old price, claim you're out of stock when you're not, or miss a service you now offer. You lose the sale and never know why.
- **Connected:** the assistant pulls your live availability and current pricing through an MCP connection and gives the customer an accurate, up-to-the-minute answer — one that can lead straight to a booking or purchase.

That's the difference between being a frozen snapshot in an AI's memory and being a live, reliable participant in AI-driven decisions. As roughly **37% of consumers now start their searches with AI** and agents move toward completing transactions, being **reachable and current** is becoming as important as being **findable**.

There's also a cost story worth knowing. Part of why 2026 is the moment for this is economics: **vertical, specialized agents are outperforming general models**, and **small language models are dramatically cheaper to run**. Cheaper, focused agents connected to real tools via MCP make it economically sensible to deploy AI against narrow business tasks at scale — which means more agents, in more places, needing to reach your data.

## What MCP means for how you expose your information

Here's the strategic reframe. For twenty years, "getting found" meant optimizing a **website for humans to read**. MCP adds a second surface: **making your data available for machines to use**.

You don't have to rebuild everything overnight, and most small businesses won't run their own MCP server first. But the mindset shift is what matters, and it's the same discipline I preach for Answer Engine Optimization:

- **Get your data clean and structured.** MCP or not, agents reward accurate, well-organized, machine-readable information. Structured product, pricing, and availability data is the raw material every AI connection depends on.
- **Understand where your platforms are heading.** Many booking systems, e-commerce platforms, and CRMs are adding MCP support so their customers' data becomes agent-reachable without custom work. Ask your vendors what their roadmap is.
- **Decide what you'd expose, and what you wouldn't.** MCP is permissioned. Think now about which information you'd want an agent to access (catalog, availability, hours, policies) versus what stays private.
- **Mind governance and security.** MCP connections are powerful, and **agent misuse is a rising security concern** while frameworks like the **EU AI Act** shape the rules. Exposing data to agents should always be scoped, logged, and permissioned — never wide open.

### A short readiness checklist

- Is my core business information (prices, availability, hours, policies) accurate and structured?
- Do my key platforms support, or plan to support, MCP or agent connectivity?
- Have I decided what an AI agent should and shouldn't be able to access?
- Am I monitoring how AI systems currently describe my business — and whether they're current?

If you can answer those, you're ahead of most.

## The bottom line

MCP isn't a product you buy, and it's not a fad to chase. It's infrastructure — the emerging standard that lets AI agents plug into the real world, your business included. You don't need to master the protocol. You need to grasp what it changes: AI is moving from **talking about** your business from memory to **working with** your live data to help customers decide and act.

The businesses that thrive in this next phase will be the ones whose information is clean, structured, and ready to be reached — the ones that treat "how do I show up to machines?" as seriously as "how do I show up to people?" MCP is the plumbing making that connection possible. Understand it now, get your data house in order, and you'll be ready when the agents come knocking. They already are.

## Key takeaways

- ② MCP (Model Context Protocol) is an open standard — think "USB-C for AI" — that gives AI agents one consistent, permissioned way to connect to external tools and live data.
- ② It solves the "custom integration for every AI-tool pair" problem: expose your data once through an MCP server and any compliant agent can reach it, with live data instead of frozen guesses.
- ② MCP powers the shift from AI that describes your business (often from stale memory) to AI that works with your current, accurate information — the same shift behind agentic commerce.
- ② Cheaper small language models and better-performing vertical agents make 2026 the year connected agents scale, meaning more agents in more places will need to reach your data.
- ② The business action isn't running a server tomorrow; it's getting data clean and structured, checking whether your platforms support MCP, and deciding what to expose.
- ② MCP connections are powerful, so governance matters — keep access scoped, logged, and permissioned amid rising agent-misuse concerns and rules like the EU AI Act.

## Frequently asked questions

### What is MCP (Model Context Protocol)?

MCP is an open standard that gives AI agents a consistent, secure way to connect to external tools and data sources. It acts like a universal adapter — often described as USB-C for AI — so any compliant agent can reach any compliant data source without a custom-built integration. It's gaining real adoption through 2026 as agents move from talking to acting.

### Why was MCP created?

On their own, AI models are frozen at their training cutoff and don't know your live prices, inventory, or availability. The old fix was hand-building a custom integration for every AI-and-tool pair, which was expensive, brittle, and impossible to scale. MCP replaces that with one standard interface, so a business exposes data once and many agents can connect to live information.

### Do I need to be technical to care about MCP?

No. You don't need to build or operate MCP yourself any more than you need to be a plumber to use running water. What matters is understanding what it changes — AI moving from guessing about your business to working with your live data — and making sure your information is clean, structured, and ready to be reached.

### How is MCP different from an API?

An API is a specific interface one developer builds for one system, and connecting AI to several tools traditionally meant many separate bespoke builds. MCP is a shared standard layered on top of that world, so agents and tools speak a common language and interoperate without a new custom bridge for every pairing. In short, MCP standardizes and scales what ad hoc APIs did one at a time.

### **Is exposing my data through MCP safe?**

It can be, because MCP is permissioned — you define exactly which data and actions an agent can access and under what limits, rather than opening your whole system. That said, agent misuse is a rising security concern and frameworks like the EU AI Act are shaping the rules, so any connection should be scoped, logged, and permissioned rather than wide open.

### **What does MCP have to do with agentic commerce?**

Agentic commerce is AI agents browsing, choosing, and buying on a person's behalf, and those agents are far more accurate and useful when they can reach live product, price, and availability data. MCP is a key way that live connection happens, letting an agent confirm current details before recommending or purchasing. So MCP is much of the plumbing that makes agent-driven buying reliable.

### **What should my business do about MCP right now?**

Start by getting your core information — prices, availability, hours, policies — accurate and structured, since clean data is the raw material every AI connection depends on. Then ask your key platforms and vendors whether they support or plan to support MCP, and decide which information you'd want an agent to access versus keep private. Most small businesses won't run their own server first; the mindset shift is what matters.

### **Will my existing software support MCP?**

Increasingly, yes — many e-commerce platforms, booking systems, and CRMs are adding MCP or agent connectivity so their customers' data becomes agent-reachable without custom development. The practical move is to ask your vendors about their roadmap and prioritize tools that are heading this direction, so you gain the benefit without building infrastructure yourself.

**About the author.** Scott Tischler is the Founder & Chairman of Alrecommend.ai and a practitioner-authority on AI search and Answer Engine Optimization. With 20+ years in marketing technology — including American Express, MetLife, and UBS — and executive study at Wharton, Harvard, Yale, and Oxford, he helps businesses become the ones AI recommends.